UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,072	08/02/2001	Glenn A. Emelko	VD7375US	5272

22203 7590 06/01/2005

KUSNER & JAFFE
HIGHLAND PLACE SUITE 310
6151 WILSON MILLS ROAD
HIGHLAND HEIGHTS, OH 44143

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 06/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/921,072	EMELKO, GLENN A.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 August 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20020708*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to because Figures 2, 3, 5, and 6 include grayscale shading which makes the labels difficult to read or illegible. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

2. The abstract of the disclosure is objected to. It is noted that the abstract includes the phrase "encryption methods such as Data Encryption Standard (DES), which rely upon the difficulty in the factorization of keys based upon large prime numbers." The Examiner further notes that although several encryption methods, notably RSA, do rely on the difficulty of the factoring problem, DES does not rely on the difficulty of factoring for its security. Correction is required. See MPEP § 608.01(b).

3. The disclosure is objected to because of the following informalities:

The specification appears to contain minor typographical and other errors. For example, on page 6, line 11, it appears that "It should understood" is intended to read "It should be understood". On page 6, lines 26-27, in the phrase "may make it cost effective to dual purpose it's use", "it's" should read "its"; further, the phrase "to dual purpose" is generally vague. On page 7, line 5, in the phrase "this is not intended to limited same", it appears that "limited" is intended to read "limit".

In the paragraph on page 11, lines 14-25, the use of trademarks, for example, ALTERA FLEX®, has been noted. The trademarks should be capitalized wherever they appear and be accompanied by the generic terminology. Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Appropriate correction is required. Applicant's cooperation is requested in correcting any other errors of which applicant may become aware in the specification.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Rao et al, "Private-Key Algebraic-Coded Cryptosystems".

In reference to Claims 1 and 5, Rao discloses an encryption method including establishing a code set having N different elements; receiving d input data symbols to be encrypted; establishing a cryptographic key including c key symbols; combining the d data symbols and the c key symbols to for a sequence of k_1 symbols; and applying an error correction encoder algorithm to the sequence of k_1 symbols, resulting in m_1 symbols of error correction information to be assigned to the sequence, in which the resulting m_1 symbols and the c key symbols are sufficient to compute the d input data symbols by applying the inverse error correction algorithm, and further in which the m_1 symbols are sufficient to error correct the d data symbols and m_1 symbols of error correction (see pages 41-43, sections 2.1, "Introduction", and 2.2, "Encryption of Modified PRAC"; also page 44, section 2.4, "Application to JOEEC").

In reference to Claims 2 and 3, Rao further discloses combining the m_1 symbols into a sequence of k_2 symbols and applying an error correction encoder algorithm to the sequence of k_2 symbols, resulting in m_2 symbols of error correction information to be received with the k_2 symbols for decryption, and in which the m_2 symbols provide error correction for the m_1 symbols (see pages 41-43, section 2.2, "Encryption of Modified PRAC").

In reference to Claim 4, Rao further discloses that the error correction encoder uses a block code, specifically for forward error correction/error correction code, namely a BCH code (see page 41, section 2.1, "Introduction", first paragraph).

In reference to Claims 6-9, Rao discloses a decryption method corresponding substantially to the encryption method of Claims 1-5 (see page 43, section 2.3 "Decryption of Modified Cryptosystems").

Claims 10-18 are directed to systems corresponding substantially to the methods of Claims 1-9, and are rejected by a similar rationale.

In reference to Claim 19, Rao discloses an encryption method including receiving input data symbols to be encrypted, establishing a key, and applying an error correction encoder algorithm to the input data symbols and the key, in which the resulting error correction symbols and the key are sufficient to determine the input data symbols by applying an error correction decoder algorithm (see pages 41-43, sections 2.1,

"Introduction", and 2.2, "Encryption of Modified PRAC"; also page 44, section 2.4, "Application to JOEEC").

In reference to Claim 20, Rao discloses a decryption method corresponding substantially to the encryption method of Claim 19 (see page 43, section 2.3 "Decryption of Modified Cryptosystems").

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Davida, US Patent 4417338, discloses a system that includes error correction encoding a key and deliberately introducing errors.

b. Riek et al, US Patent 5054066, discloses a cryptographic method that includes the use of a linear code.

c. Jiawook et al, US Patent 6125183, discloses a cryptosystem that includes the use of error detection and correction using an algebraic code, specifically a Reed-Solomon code.

d. Schneier, *Applied Cryptography*, describes cryptographic algorithms based on error-correction codes.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-

3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER